TATA CONSULTANCY SERVICES

Building on belief

IBM Qradar SIEM

10/04/2022

Building on belief

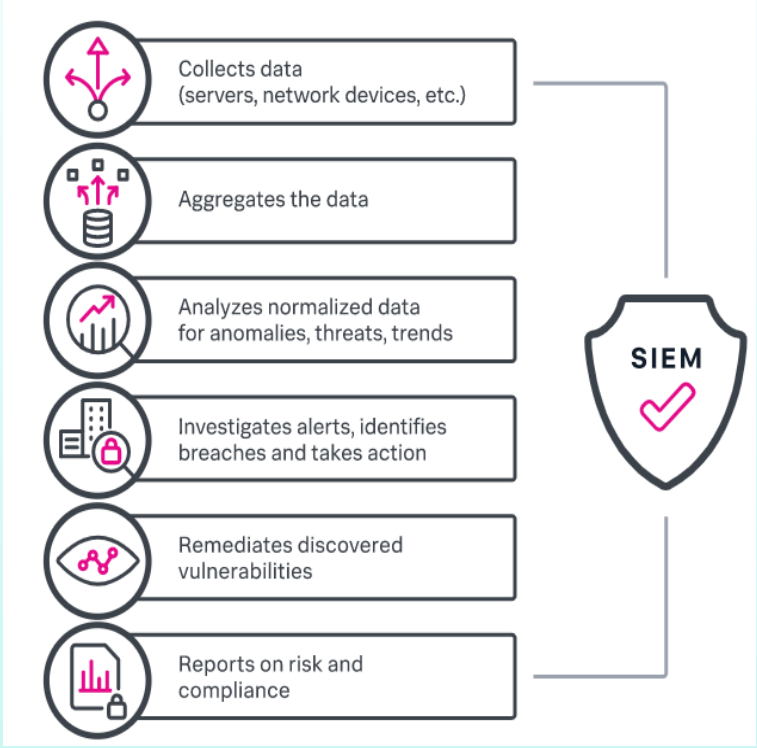
What is SIEM

Security information and event management (SIEM) is basically a cybersecurity technology that provides a single, streamlined view of your data, insight into security activities, and operational capabilities so we can effectively detect, investigate and respond to security threats.

A SIEM solution aggregates event data across disparate sources within our network infrastructure, including servers, systems, devices and applications, from perimeter to end user, and including cloud and hybrid environments, as well as on-premises.

Ultimately, a SIEM solution offers a centralized view with additional insights, combining context information about users, assets and more.

It consolidates and analyzes the data for deviations



TATA CONSULTANCY SERVICES

Building on belief

IBM Qradar SIEM

- IBM QRadar Security Information and Event Management (SIEM) helps security teams detect, prioritize and respond to threats across the enterprise. It automatically aggregates and analyzes log and flow data from thousands of devices, endpoints and apps across your network, providing single, prioritized alerts to speed incident analysis and remediation

- IBM QRadar collects, processes, aggregates, and stores network data in real time. QRadar uses that data to manage network security by providing real-time information and monitoring, alerts and offenses, and responses to network threats.

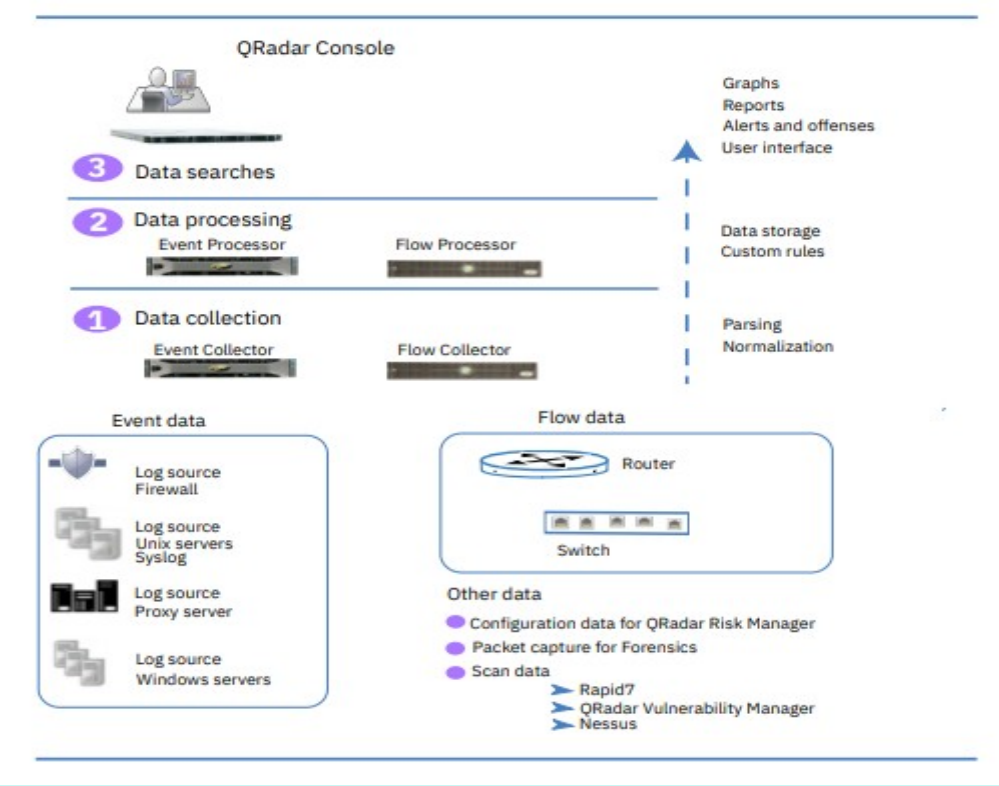
- The Solution uses a combination of flow-based network knowledge, security event correlation, and asset-based vulnerability assessment.

TATA CONSULTANCY SERVICES

Building on belief

Basic Qradar Architecture

The following three layers that are represented in the diagram are the core functionality of any QRadar system



Three layers of QRadar security intelligence platform:

1.DATA COLLECTION

- Data collection is the first layer, where data such as events or flows is collected from your network. The All-in-One appliance can be used to collect the data directly from your network or you can use collectors such as QRadar Event Collectors or QRadar QFlow Collectors to collect event or flow data.

- The data is parsed and normalized before it passed to the processing layer. When the raw data is parsed, it is normalized to present it in a structured and usable format.

- Event data represents events that occur at a point in time in the user's environment such as user logins, email, VPN connections, firewall denys, proxy connections, and any other events that you might want to log in your device logs.

- Flow data is network activity information or session information between two hosts on a network, which QRadar translates in to flow records. QRadar translates or normalizes raw data in to IP addresses, ports, byte and packet counts, and other information into flow records, which effectively represents a session between two hosts.

- ***2.DATA PROCESSING***

  the second layer or data processing layer is where event data and flow data are run through the Custom Rules Engine (CRE), which generates offenses and alerts, and then the data is written to storage.

  Event data, and flow data can be processed by an All-in-One appliance without the need for adding Event Processors or Flow Processors. If the processing capacity of the All-in-One appliance is exceeded, then you might need to add Event Processors, Flow Processors or any other processing appliance to handle the additional requirements.

- ***3.DATA SEARCHES***

  In the third or top layer, data that is collected and processed by QRadar is available to users for searches, analysis, reporting, and alerts or offense investigation.

  Users can search and manage the security admin tasks for their network from the user interface on the QRadar Console.

CRE(custom rule Engine)

It is responsible for processing events that are received by QRadar and comparing them against defined rules.

The Custom Rules Engine (CRE) displays the rules and building blocks that are used by IBM QRadar. Rules and building blocks are stored in two separate lists because they function differently.

The CRE provides information about how the rules are grouped, the types of tests that the rule performs, and the responses that each rule generates.

As event and flow data passes through the CRE, it is correlated against the rules that are configured and an offense can be generated based on this correlation

ACCUMULATION

The Accumulator is a QRadar process that counts and prepares Events and Flows in data accumulations to assist with searches, displaying charts, and report performance.

Accumulated Data is an aggregate data view used to draw a Time Series graph or run Scheduled Reports

The Accumulator service runs on all appliances with local storage to create the minute-by-minute accumulations

Device Support Module (DSM)

IBM QRadar uses Device Support Modules (DSMs) to log and correlate the data that is collected from external log sources, such as firewalls, switches, or routers.

DSMs are regularly updated to ensure that QRadar can correctly interpret and parse security event information that is provided by external devices. DSMs can be updated both automatically and manually.

Although QRadar devices include native log sending capabilities, several devices require extra configuration, or an agent, or both, to send logs. Configuration varies between device types. You must ensure that the devices are configured to send logs in a supported format.

QRadar can receive logs from systems and devices by using the Syslog protocol, which is a standard protocol. Supported DSMs can use other protocols.

TATA CONSULTANCY SERVICES

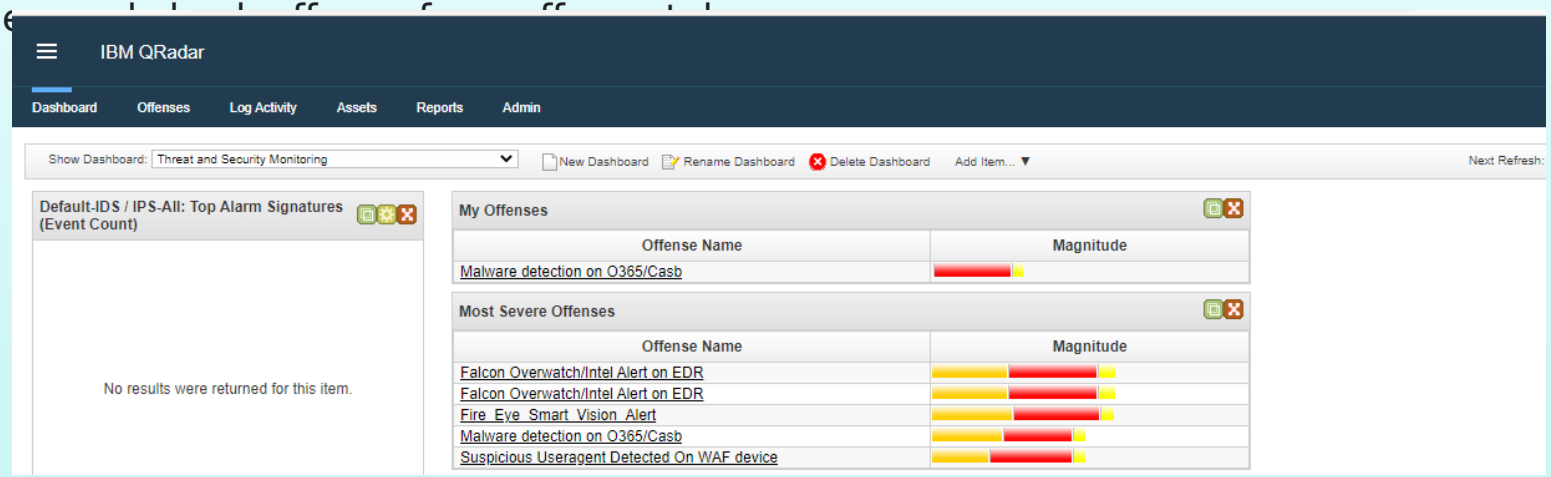
Building on belief

Qradar Console Overview:

The QRadar UI Console provides us access to different tabs like real-time event and flow views, reports, offenses, asset information, and administrative functions.

We can view different dashboards or can manually create new dashboard as per our requirement.

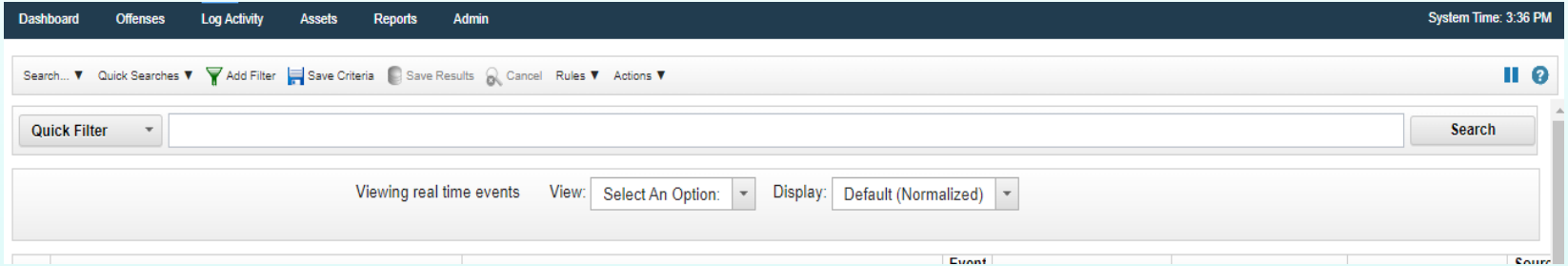
We can vie



TATA CONSULTANCY SERVICES

Building on belief

How to Run search queries on Qradar Console:



In IBM Qradar, we can perform searches on the Log Activity and Offenses tabs

You can specify filter criteria to search for events, flows, and offenses. After you perform a search, you can also save the search criteria and the search results.

Quick filter is one of the fastest methods that you use to search for event or flow payloads for specific data.

We can create a customized search by doing search for data that match our criteria by using more specific search options. You can specify columns for your search, which you can group and reorder to efficiently browse your search results.

- ***Offense management and its features:***

  IBM QRadar uses rules to monitor the events and flows in network to detect security threats. When the events and flows meet the test criteria that is defined in the rules, an offense is created to show that a security attack or policy breach is suspected.

  IBM Qradar reduces billions of events and flows into a manageable number of actionable offenses that are prioritized by their impact on our business operations.

  The magnitude rating of an offense is a measure of the importance of the offense. QRadar uses the magnitude rating to prioritize offenses and helps to determine which offenses to investigate first.

  Offense indexing provides the capability to group events or flows from different rules indexed on the same property together in a single offense.

  As per the offense severity, Triggered offenses are assigned to available shift engineers for further investigation

TATA CONSULTANCY SERVICES

Building on belief

Thank You

10/04/2022